SECURE BRANCH CONNECTIVITY

SUMMARY

Internet downtime is a problem. However, when we talk about enterprise networks and connecting dozens or hundreds of business branches into a secure internal network, the problem of Internet downtime becomes a significant financial loss. In fact, according to Appdynamics and Cisco, small businesses can expect 1 hour of downtime to cost $8580 whereas medium businesses are subject to even more substantial costs of $215 637 per hour. These numbers look astronomical, but we must take into consideration that they take into account the loss of customer confidence and that enterprises nowadays are very distributed and rely on complex internal systems to make sure they are operational.

CHALLENGE

The world of enterprise networking has been experiencing a change in perception lately due to newly available technologies to access the Internet. Traditionally, wired internet options, such as DSL or fiber, are the most popular, but they cannot ensure 100% Internet availability, due to unavoidable causes such as equipment failure or power outages. It is essential to highlight that even 99% of uptime results in 3.65 days/year during which Internet services are not available. If we take this into account and calculate potential losses for widespread enterprise business it is evident that even 99% of uptime provided by traditional enterprise Internet access options is not good enough. Because of this, businesses around the world are turning to 4G LTE to provide secure and dependable backup or even primary branch connectivity.

SOLUTION

The topology presented in this use case focuses on a challenge when the headquarters of an enterprise needs to be reliably connected to a branch using encrypted VPN data channels. The headquarters has a wired WAN link with cellular backup provided by RUTX09 – an enterprise router with LTE-A connectivity and advanced RutOS features for security and remote management, such as support for DMVPN, MQTT & SNMP, and others. Then, workplaces are connected using another device from Teltonika Networks X series – the RUTX08, which is a professional Ethernet-to-Ethernet router offering excellent VPN performance and same remote management capabilities as the RUTX09. Finally, RUTX10 brings AC Wi-Fi (2.4 GHz + 5GHz) wireless connectivity service to areas such as meeting rooms, where it is essential to quickly connect to internal systems and offer separate public hotspots for visitors with different access and security settings applied in comparison to internal enterprise user network.

TOPOLOGY
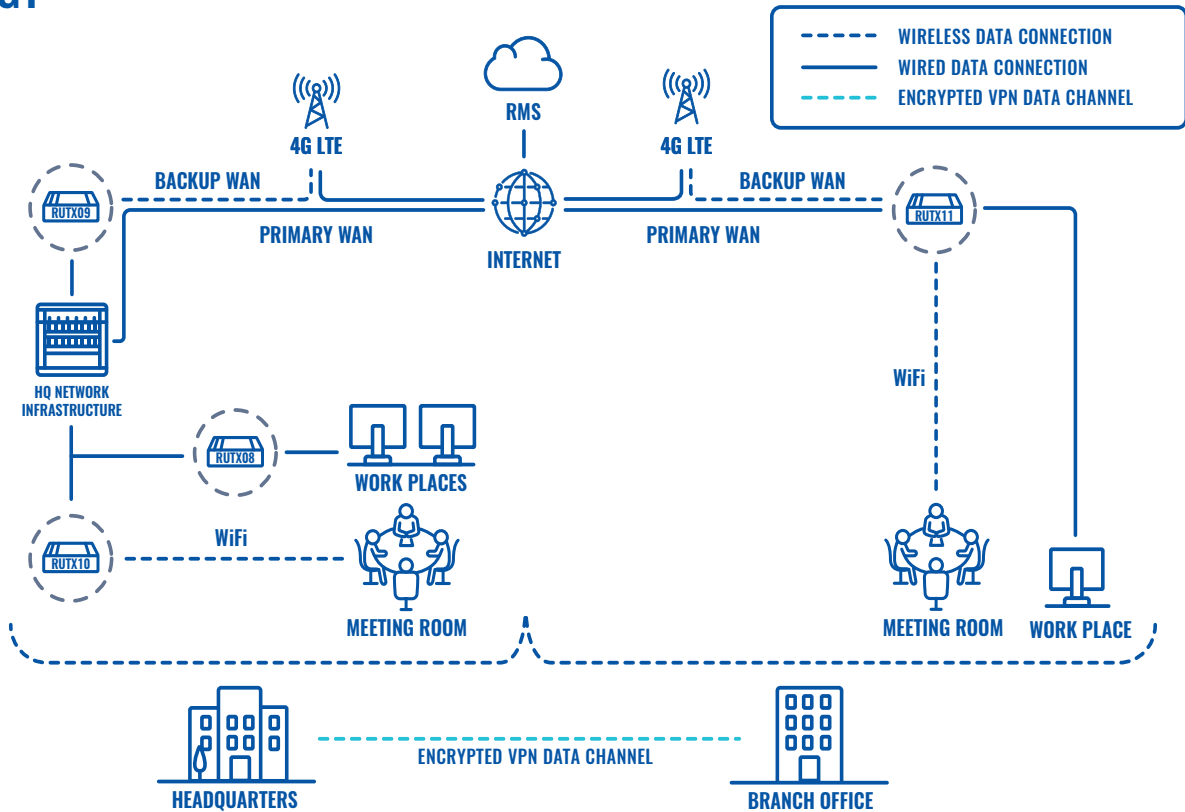
On the branch side, RUTX11 offers all needed connectivity through LTE-A with a maximum throughput of 300Mbps and shares it using Gigabit Ethernet and AC Wi-Fi interfaces. Using RUTX11 as the primary Internet source enables business to scale quickly, enabling 1-day connectivity with no delays for obtaining wired Internet source, which in practice can take weeks, if not months.

BENEFITS

• Teltonika X series cellular routers (X11 & X09) offer LTE – Advanced connectivity with speeds up to 300 Mbps and Carrier Aggregation – sufficient to replace aging and unreliable wired WAN options.

• Also, X11 & X10 offers AC Wi-Fi able to offer wireless service using 2.4 GHz & 5 GHz frequency channels, which allows for faster service and separation of private/public hotspots.

• All RUT X series routers are compatible with RMS, which allows to monitor performance with customizable reports & alerts, manage configurations of devices, and much more – remotely, even without Public IP!

WHY TELTONIKA?

X series routers by Teltonika Networks come in 4 different configurations with or without cellular & Wi-Fi, meaning that you can use devices from the same series across enterprise networking infrastructure, ensuring maximum compatibility, but staying cost-efficient. Even better, all RUT X series routers support remote monitoring and management by the Teltonika Remote Management System (RMS), which is a highly secure & robust cloud platform that helps system operators to control unlimited amount of Teltonika Networks equipment from anywhere, even without Public IP.